Zidong Zhang

Email: zza323@sfu.ca

Research Interest

SAST (Static application security testing) on Mobile System/Web Applications; Security and Privacy of Mini-Program Ecosystem; BLE Security.

Education

- **Simon Fraser Univerisity** — Burnaby, BC, Canada
  Phd. Student of Computer Science; — *Sept 2024 - June 2028 (expected)*
  Advisor: *Prof.Jianliang Wu*
- **Shandong Univerisity** — Qingdao, China
  Master of Cybersecurity and Information Security; GPA: 86/100 — *Sept 2021 - June 2024*
  Advisor: *Prof.Wenrui Diao*
- **Hebei Univerisity** — Baoding, China
  Bachelor of Information Security; GPA: 3.91 — *Sept 2017 - June 2021*
  GPA Ranking: *9/110 (Top 8%)*
- **Boston Univeristy** — Boston, MA, USA
  Visiting Student; — *Jan 2020 - Feb 2020*

Publications

**: Co-first Author*

- **How Bad Can It Be: Detection and Measurement of Crypto API Misuse in Open-Source Ecosystems**
  Xiangfan Wu, Lingyun Ying, Huajun Chai, **Zidong Zhang**, Haipeng Qu, Haixin Duan
  Under Submission
- **Hey, Your Secrets Leaked! Detecting and Characterizing Secret Leakage in the Wild**
  Jiawei Zhou*, **Zidong Zhang***, Lingyun Ying, Huajun Chai, Jiuxin Cao, Haixin Duan
  IEEE Symposium on Security and Privacy 2025 (IEEE S&P 2025)
  Accept Rate: 14.8%
- **MiniCAT: Understanding and Detecting Cross-Page Request Forgery Vulnerabilities in Mini-Programs**
  Zidong Zhang, Qinsheng Hou, Lingyun Ying, Yacong Gu, Rui Li, Wenrui Diao, Shanqing Guo, Haixin Duan
  The ACM Conference on Computer and Communications Security (ACM CCS 2024)
  Accept Rate: 16.9%
- **MiniBLE: Exploring Insecure BLE Implementation in Mini-Programs**
  Zidong Zhang, Jianqi Du, Wenrui Diao, Jianliang Wu.
  ACM Workshop on Secure and Trustworthy Superapps (SaTS 2024). Co-located with ACM CCS 2024.
- **Living in the Past: Analyzing BLE IoT Devices Based on Mobile Companion Apps in Old Versions**
  Jianqi Du, **Zidong Zhang**, Fenghao Xu, Wenrui Diao
  The 19th International Conference on Mobility, Sensing and Networking (IEEE MSN 2023)
- **Identifying the BLE Misconfigurations of IoT Devices through Companion Mobile Apps [Link]**
  Jianqi Du, Fenghao Xu, Chennan Zhang, **Zidong Zhang**, Xiaoyin Liu, Pengcheng Ren, Wenrui Diao, Shanqing Guo, Kehuan Zhang.
  The 19th Annual IEEE International Conference on Sensing, Communication, and Networking (IEEE SECON 2022)

Research Experience

- **QI-ANXIN Research Institute** — Beijing, China
  Security Researcher Intern; Advisor: Dr.Lingyun Ying & Dr.Yacong Gu — *Oct 2022 - Now*
  - **Mini-Program Analyzing:** Built a mini-programs crawler to crawl 130,000 apps and carried out a large-scale automated measurement for routing security vulnerabilities in mini-programs by using hybrid analysis.
  - **SAST for JavaScript:** Built the static automated vulnerability detection for JavaScript-based applications (e.g., mini-programs) using CodeQL.
  - **Smart IoT Device Security:** Analyzed the protocol and verification process of smart locks and implemented the takeover of any of its devices through its companion mini-programs.
  - **Secrets Leakage Detection:** Design Automated Secrets Detection tools to conduct large-scale measurement among Github, Pypi and Wechat Mini-program to find leaked secrets in the wild.

Projects

- **Automated Detection of Mini-Program Vulnerabilities with Hybrid Analysis**
  - Discovered a novel security vulnerability in mini-programs with their routing implementations for the first time.
  - Performed an automated large-scale static analysis of 130,000 mini-programs with CodeQL while using the Xposed Hook for dynamic verification.
  - **Accomplishments:** One paper accpted(ACM CCS '24); One paper in submission (SaTS' 24); 3 vulnerabilities confirmed by CNVD.
- **Analyzing BLE Devices with Older Versions of Companion Apps**
  - Analyzed BLE devices that could not be OTA upgraded via old version of their companion apps.
  - Designed an automated tool to perform large-scale automatic measurements in IoT App datasets to measure the security risks from older versions of apps for devices that do not support OTA upgrades.
  - **Accomplishments:** One paper accepted (IEEE MSN '23); 3 vulnerabilities under CVE review.
- **Identifying the BLE Misconfigurations of IoT Devices through Companion Apps**
  - Based on the static analysis, defined a set of strategies for detecting misconfiguration in the companion app of BLE devices.
  - Designed an automatic analysis tool to detect the BLE misconfigurations based on pre-defined checking strategies from 4,589 companion apps.
  - **Accomplishments:** One paper published. (IEEE SECON '22)

Teaching

- **Teaching Assistant** Qingdao, China
  - **Software Security:** Instructor: Prof.Wenrui Diao (2021 Fall)
  - **Reverse Engineering:** Instructor: Prof.Wenrui Diao (2023 Spring)

Professional Activities

- USENIX Security Symposium (USENIX SEC): Artifact Evaluation Committee (AEC) Member, 2025; External Reviewer, 2025
- ACM Conference on Computer and Communications Security (ACM CCS): External Reviewer, 2024, 2025
- ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS):External Reviewer, 2025
- IEEE European Symposium on Security and Privacy (IEEE EuroS&P):External Reviewer, 2024
- International Conference on Information Security and Cryptology (Inscrypt): Subreviewer, 2023
- CCF Chinasoft: Subreviewer, 2023
- International Conference on Information and Communications Security (ICICS): Subreviewer, 2022
- European Symposium on Research in Computer Security (ESORICS): Subreviewer, 2022

Honors and Awards

- ACM CCS 2024 Travel Grant - Oct. 2024
- DataCon Security Analysis Competition, Vulnerability Analysis Track, Third Place (3/689 teams) - Nov. 2023
- The Mathematical Contest in Modeling (MCM), Meritorious Winner - April 2020
- National College Student Information Security Contest (CISCN), First Prize of North China Region - Sept. 2020
- National College Student Information Security Contest (CISCN), Second Prize of North China Region - June 2019
- College Student Information Security Contest in Hebei Province, First Prize - October 2019

Vulnerabilities Disclosures

- WeChat Mini Program Privilege Escalation Vulnerability. (CNVD-2023-75836, CNVD-2023-75837)
- Nankai University Original Vulnerability Reporting Certificate. (EDUSRC-NKU-2019-0074)
- Shanghai Jiaotong University Original Vulnerability Reporting Certificate. (EDUSRC-2019-0217)
- Shanghai International Studies University Original Vulnerability Reporting Certificate. (SISUVD-2019074)

Technical Skills

- **Development:** Python, PHP, JavaScript, Lua, C++, BLE Development (for Android).
- **Security tools:** CodeQL, Xposed, Frida, Android Reverse(Jadx), IDA Pro, Burpsuite, Nmap, Metasploit.